IDOR (Insecure Direct Object Reference)

```
IDOR  (Insecure direct object references )


https://example.com/?id=2


DELETE /file=ahmed.txt => ali.txt
```

- ال IDOR هيا انك تقدر توصل لحاجات مش مسموح ليك انك توصلها
- مثلا انت ف ملف اسمو YYYY.txt بيظهر ف الرابط الـ Path لو انت غيرته قدرت توصل لملف تاني تبقي كدا في IDOR
- او لو انت مثلا ليك ID ف الموقع 123 واللي بعدك ليه 124 وهكذا لو انت غيرت ال ID بتاعك ل 124 وقدرت توصل ليه تبقي كدا IDOR

> **Note**
>
> - تخيل إنك داخل على موقع بنك، وده رابط كشف حسابك:

`https://bank.com/account?user_id=1234`

فانت رقمك كمستخدم هو 1234، والموقع بيعرض بياناتك بناءً على الرقم ده.

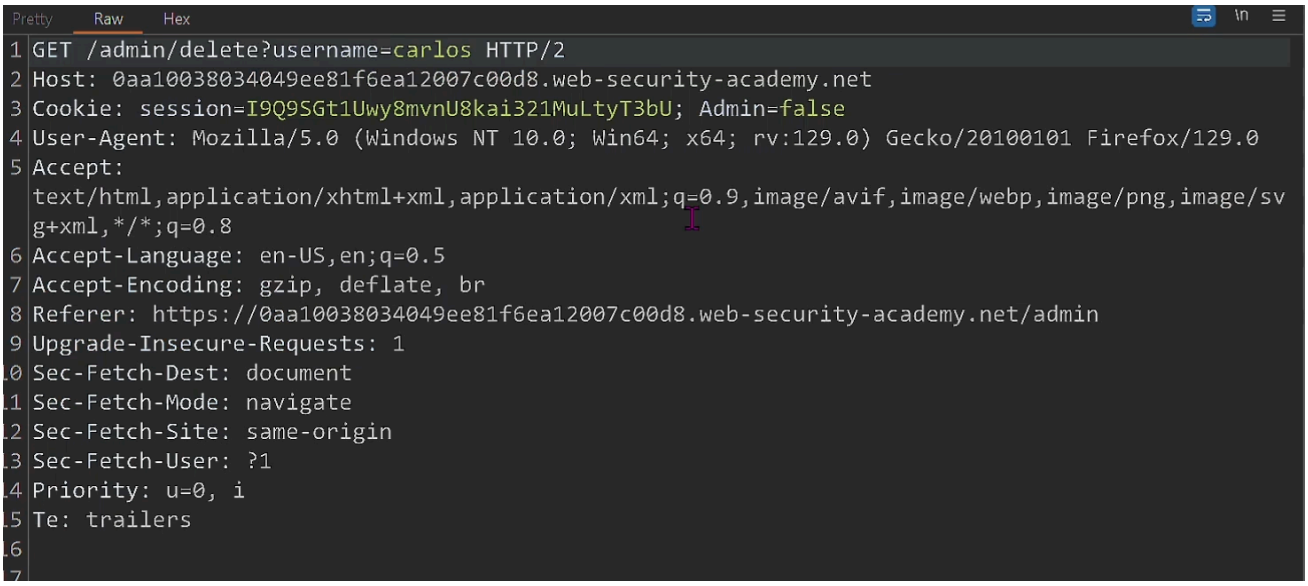
لكن تخيل لو أي حد غيرك غيّر الرقم ده في الرابط كده:

`https://bank.com/account?user_id=1235`

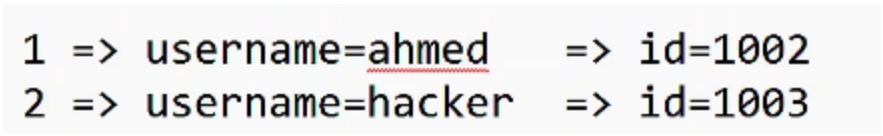
وفجأة ظهرت له بيانات شخص تاني!
كده الموقع مصاب بثغرة **IDOR**، لأنه ما تحققش هل المستخدم اللي طالب البيانات فعلاً عنده الحق يشوفها.

```
https://example.com?username=mohamed => chat mohamed
```

- مش ID بس ممكن تغير ف اسم ال USER برضو



- ممكن تحاول تخش ك admin وتوقف الطلب وتغير ال False لـ True
- هتبقي ادمن ومعاك صلاحيات اعلي



- وانت بتعمل الثغره دي علشان تجربها انت تعمل اكونتين
- وبتعرف ال id وكل حاجه
- تخش علي ال burp وتحلل ال Requets وتشوف لقيتو بيرجعلك الـ username غيره باسم الاكونت التاني
- لقيتو بيرجع ال id حط id الاكونت التاني